

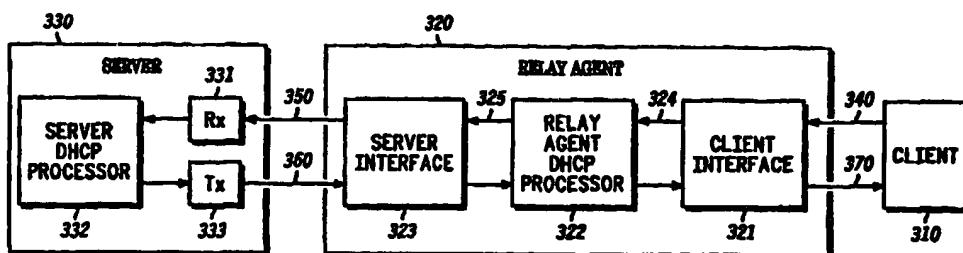


INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04J 3/02, 3/14, H01J 13/00	A1	(11) International Publication Number: WO 98/26530 (43) International Publication Date: 18 June 1998 (18.06.98)
---	----	--

(21) International Application Number: PCT/US97/22006	(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).
(22) International Filing Date: 3 December 1997 (03.12.97)	
(30) Priority Data: 60/032,482 9 December 1996 (09.12.96) US 08/972,865 18 November 1997 (18.11.97) US	
(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).	Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>
(72) Inventors: PATRICK, Michael, W.; 9 Elizabeth Drive, Assonet, MA 02702 (US). FLETCHER, James, A.; 12 Connie Drive, Foxboro, MA 02035 (US).	
(74) Agents: WOOD, J., Ray et al.; Motorola Inc., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196 (US).	

(54) Title: SYSTEM, DEVICE, AND METHOD FOR ROUTING DHCP PACKETS IN A PUBLIC DATA NETWORK

300

(57) Abstract

A system (300), device (320, 330) and method (200) for routing DHCP packets in a public data network wherein a relay agent inserts a source identifier into DHCP request packets. A server extracts the source identifier from the DHCP request packets and inserts the information into DHCP response packets. The relay agent uses the information to determine a destination for the DHCP response packets.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon	KR	Republic of Korea	PL	Poland		
CN	China	KZ	Kazakhstan	PT	Portugal		
CU	Cuba	LC	Saint Lucia	RO	Romania		
CZ	Czech Republic	LI	Liechtenstein	RU	Russian Federation		
DE	Germany	LK	Sri Lanka	SD	Sudan		
DK	Denmark	LR	Liberia	SE	Sweden		
EE	Estonia			SG	Singapore		

**System, Device, and Method For Routing DHCP Packets
in a Public Data Network**

Background

5 **1. Field of the Invention**

The invention relates generally to communication systems and, more particularly, to routing DHCP packets in a public data network.

10 **2. Discussion of Related Art**

In today's information age, there is an increasing need for high speed communications that provides access to on-line services for an ever-increasing number of communications consumers. To that end, communications networks and technologies are evolving to meet current and future demands. Specifically, new networks are being deployed which reach a larger number of end users, and protocols are being developed to utilize the added bandwidth of these networks efficiently.

One protocol that is used pervasively in modern communications networks including "the Internet" is the Internet Protocol (IP). IP provides "connectionless" service in that each unit of IP information (referred to as a datagram) is routed from its source to its destination according to an IP address in the datagram without reference to any pre-established physical or virtual connection between the source and the destination. IP is also considered to be an unreliable protocol, since it does not guarantee that all datagrams will be delivered to their destinations and does not guarantee that datagrams will be delivered in the order in which they were sent.

Although IP is connectionless and unreliable, it provides a flexible platform over which other higher-layer protocols can be carried. One such protocol is the Transmission Control Protocol

(TCP), which provides connection-oriented reliable service over the IP protocol. TCP is the most common protocol used with IP, and together they are often referred to as TCP/IP.

- Each device that will use IP services must have a unique IP address. In many cases, a device will be pre-assigned an IP address. However, in some cases, it is impractical or undesirable to pre-assign IP addresses. For example, if a particular location has a large number of devices that use IP services, but only a small number will be using IP services simultaneously, it would be a waste of IP addresses to pre-assign a unique IP address to each device. Instead, it is preferable to assign IP addresses as needed from a pool of IP addresses. Dynamic assignment of IP addresses simplifies client configuration and conserves IP addresses by assigning addresses only to actively connected clients.
- One protocol for dynamically assigning IP addresses is the Dynamic Host Configuration Protocol (DHCP) which is described in the Internet Engineering Task Force (IETF) RFC 1541. DHCP allows a client that wishes to use IP services to obtain an IP address from a server that maintains a pool of IP addresses. DHCP works generally as follows. When the client needs an IP address, it broadcasts a DHCP-Discover packet into the network. One or more servers receive the DHCP-Discover packet and respond with a DHCP-Offer packet including an IP address for the client. Since the client may receive multiple offers, the client accepts one of the offers and broadcasts a DHCP-Request packet indicating which DHCP-Offer was accepted. The server which made the offer then broadcasts a DHCP-Ack packet to the client containing configuration parameters for the client.
- In typical local-area networks (LANs), the client and the server are on the same LAN segment, so the broadcast messages are handled locally by the client and the server. However, when the client

accesses the server over a wide-area network (WAN), such as a hybrid fiber-optic/coaxial cable (HFC) network, the broadcast messages must be routed by one or more intermediate relay agents.

One problem caused by the routing function is that the
5 broadcast messages must be transmitted on all network segments supported by the relay agent, since the relay agent cannot determine a unique destination for each message. Furthermore, all devices on the network receive the broadcast messages and must process them, even if the processing is only to determine that the messages can be
10 ignored. Thus, the broadcasting of DHCP messages, and in particular the broadcasting of DHCP responses from the server to the client, waste network bandwidth and waste processing resources in non-participating devices.

Thus, a need remains for an apparatus and method for
15 intelligently routing DHCP packets.

Brief Description of the Drawing

In the Drawing,

FIG. 1 shows an exemplary TCP/IP network as is known in the
20 art;

FIG. 2 is a flow diagram of a method for routing DHCP packets;
and

FIG. 3 shows a system for routing DHCP packets.

25

Detailed Description

As discussed above, the need remains for an apparatus and method for intelligently routing DHCP packets. This invention routes DHCP response packets to only the network segment on which the
30 initiating client is located. The relay agent is able to determine the

destination network segment by inserting a source identifier into the DHCP packets sent by the client and receiving the source identifier back from the server in DHCP packets sent by the server.

FIG. 1 shows an exemplary TCP/IP network 100 as is known in the art. In this example, client devices access on-line services such as the Internet and a DHCP server by means of a wide-area network (WAN). Each client interfaces with the WAN by means of a modem which provides physical layer connectivity to a Headend Unit.

Headend Unit typically supports a number of modems over a number of physical modem connections. Headend Unit terminates the physical modem connections and relays IP datagrams between the clients and the on-line services. Thus, one of the functions of the Headend Units is to act as the relay agent for DHCP packets.

Where the Headend Unit supports a number of physical modem connections, any broadcast messages sent by an on-line service must be transmitted by the Headend Unit over all physical modem connections. As discussed above, this broadcast transmission is wasteful of WAN network resources. Also as discussed above, this broadcast transmission is wasteful of client processing resources.

This problem is solved by including a source identifier in DHCP messages that is then used by the relay agent to identify the destination physical modem connection. Although this information could be added by the client itself, the client is considered to be an untrusted device which could insert false information to cause network problems or obtain unauthorized services. A preferred embodiment has the relay agent itself insert the source identifier into DHCP packets sent by the client. The relay agent is considered to be secure since it is typically within the control of the service provider as opposed to the client which is typically within the control of the end user.

The relay agent can insert any information that is has available for identifying the physical modem connection, including (but not limited to) a client identifier, a modem identifier, and a circuit identifier. The source identifier is returned by the server in any 5 DHCP packets it sends. The relay agent uses the source identifier to route DHCP responses to the correct physical modem connection.

FIG. 2 is a flow diagram of a method for intelligently routing DHCP packets in a network having a client connected to a server by means of a relay agent. The method begins with the client sending a 10 DHCP request packet. Upon receipt of the packet by the relay agent, the relay agent inserts a source identifier into the packet and forwards the modified packet to the server. Upon receipt of the modified packet, the server formats a DHCP response packet including the source identifier received in the request packet and forwards the 15 response packet to the relay agent. Upon receipt of the response packet, the relay agent uses the source identifier to determine which one of a number of communications links is the destination for the response packet. The relay agent then sends the response packet on the destination communications link to the client.

FIG. 3 shows a system 300 for routing DHCP packets in accordance with the present invention. The system 300 includes a client 310 which generates a DHCP request packet. The DHCP request packet is sent to a relay agent 320 over an interface 340. The relay agent 320 inserts information into the DHCP request packet to form a 25 modified DHCP request packet. The modified DHCP request packet is sent to a server 330 over an interface 350. In one embodiment, the information is a source identifier.

The server 330 receives the modified DHCP request packet over interface 350 and extracts the information from the packet. In one 30 embodiment, the server uses the information locally in selecting an

IP address and other information for the client. In another embodiment, the server inserts the information into a DHCP response packet which it sends to the relay agent 320 over interface 360.

- The relay agent 320 receives the DHCP response packet
- 5 containing the information and extracts the information from the packet. In one embodiment, the relay agent 320 uses the information to determine a destination for the DHCP response packet. The relay agent 320 sends the DHCP response packet to the client over interface 370.
- 10 The relay agent 320 includes a client interface 321 for receiving DHCP request packets from the client. The relay agent 320 also includes a relay agent DHCP processor 322 which receives DHCP request packets from the client interface 321 over interface 324 and inserts information into the DHCP request packets to form modified
- 15 DHCP request packets. The relay agent DHCP processor 322 outputs the modified DHCP request packets to a server interface 323 over interface 325. The server interface 323 sends the modified DHCP request packets to the server 330.

- The server interface 323 also receives DHCP response packets
- 20 from the server which include the information inserted by the server 330. In one embodiment, the information in the DHCP response packet is equal to the information in the modified DHCP request packet. The relay agent DHCP processor 322 uses the information, for example, to determine a destination for the DHCP response packets. The client
- 25 interface 321 sends the DHCP response packets to the destination client.

- The server 330 processes DHCP request packets containing information inserted by the relay agent 320. The server 330 includes a receiver 331 for receiving the DHCP request packets, a server DHCP
- 30 processor 332 for extracting the information and for processing the

DHCP request packet, and a transmitter 333 for sending a DHCP response packet including the information inserted by the relay agent.

The operation of having the relay agent insert information into DHCP packets is useful for solving other problems that arise when

5 using DHCP over a public data network. As discussed above, the relay agent can insert any information it has available. Thus, the relay agent can insert other types of information in addition to or in place of a source identifier. The server and relay agent can then use the inserted information to provide security and other services.

10 One service that the relay agent can provide is protection against IP address spoofing. IP address spoofing occurs when a client uses an unauthorized IP address. By spoofing an improper IP address, the client either denies service to a legitimate user or attempts to bypass address-based access controls within the network. The relay 15 agent protects against this attack by maintaining a list of the IP addresses assigned by the DHCP server and only forwarding those IP addresses that have been assigned by the DHCP server.

Another service that the relay agent can provide is to allow multiple clients connected to the same modem to be assigned IP

20 addresses from the same Logical IP Subnet (LIS). It is desirable for all clients attached to the same modem to have IP addresses from the same LIS so that the clients will be able to use the Address Resolution Protocol (ARP) to determine the MAC addresses of other clients on the same LAN, enabling direct client-to-client 25 communication. If the clients are permitted to be assigned IP addresses from different LISs, then communication between two clients on the same LAN would require routing of all information over the WAN to the relay agent and back over the WAN to the destination client. The relay agent solves this problem by remembering the LIS 30 for the first IP address assigned to a client supported by a particular

modem, and then inserting that LIS into DHCP packets sent by other clients supported by the same modem.

Yet another service that the relay agent can provide is to allow multiple LISs to be supported in the network. In general, a number of

5 non-contiguous LISs may be assigned for allocation by the network.

The issue then becomes which LIS to use for determining the contents of the "giaddr" which is a field that is included in packets sent to servers for identifying the relay agent from which the packet was generated. Normally, relay agents set the "giaddr" to the IP address

10 of the interface on which the client request was received. However, in networks such as the network depicted in FIG. 1 above, the interfaces on the relay agent over which client packets are received

do not have IP addresses (they are termination points for physical connections and generally are not IP addressable). Since each

15 physical modem link may support multiple modems, and each modem may support multiple clients having multiple LISs, there may be a number of LISs all of which are associated with a single physical modem link. One embodiment has the relay agent use a single LIS for all "giaddr" settings. However, this is an unnecessary

20 oversimplification which is avoided by having the relay agent select from among the number of LISs, for example, using a round-robin technique for selecting an LIS.

One service that the server can provide is protection against IP address exhaustion. IP address exhaustion can occur when a single

25 client requests multiple IP addresses until the pool of IP addresses is exhausted. Such an attack can be used to maliciously deny service to other users. The server protects against this attack by maintaining a list of the clients (using the source identifier information inserted by the relay agent) and denying an IP address to

30 any client that requests more than one IP address.

Another service that the server can provide is the configuration of subnets. The original IP version 4 specification called for "classed" addresses, whereby the subnet mask of an IP address could be determined by the address itself. For some time now, however, an explicit subnet mask has been required for IP interface configuration, in order to implement "classless" IP subnetwork number assignment.

The DHCP protocol provides no mechanism for the DHCP relay agent to provide the subnet mask of the interface from which it received the original request from the client. The DHCP server, however, must know what the subnet mask is in order to select the proper range of host addresses for assigning the client an IP address. In the absence of subnet mask information, the DHCP server must either use a mask that can be implied from other addressing information or, more commonly, rely on pre-configured information of the subnet structure from which to assign addresses. However, pre-configuration of subnet information can be tedious considering the huge number of devices that may have different subnet masks. To solve this problem, the relay agent inserts the subnet mask of the interface from which it received the original request from the client, and the server uses the subnet mask to choose an IP address from the pool of IP addresses within the specified subnet.

In order to support the above-mentioned services, the relay agent must insert information such as an Agent Circuit ID, an Agent Remote ID, and an Agent Subnet Mask into DHCP packets. However, the format of DHCP packets as specified in IETF RFC 1541 does not include fields for inserting such information. Therefore, extensions in the form of numbered DHCP options are necessary to the DHCP specification to allow such information to be inserted. Each DHCP option includes a code field to identify the option, a length field, and a data field for carrying the option information. Code field numbers

are assigned by a standards body within the IETF. Code field numbers for an Agent Circuit ID option, an Agent Remote ID option, and an Agent Subnet Mask option have been assigned the decimal values 82, 83, and 84, respectively. The following is a description of an

5 embodiment of the extended DHCP options. Specific option field formats (including the assigned code field numbers) will be presented to the IETF for adoption as a standard, although proprietary formats may be used, and the invention is not limited to or by the formats of the option fields.

10 An Agent Circuit ID MAY be added by DHCP relay agents which terminate switched or permanent circuits. It encodes a agent-local identifier of the circuit from which a DHCP discover/request packet was received. It is intended for use by agents in relaying DHCP responses back to the proper circuit. Possible uses of this field

15 include:

- Router interface number
- Switching Hub port number
- Remote Access Server port number
- Frame Relay DLCI

20 - ATM virtual circuit number

- Cable Data virtual circuit number

DHCP relay agents SHALL NOT modify any existing Agent Circuit ID which may be in a received DHCP Discover/Request packet; such an option may have been added by a circuit bridge.

25 DHCP servers supporting this option MUST return the option value unchanged in all Offer and Ack responses. Servers MAY use the information for IP and other parameter assignment policies.

An Agent Remote ID MAY be added by DHCP relay agents which terminate switched or permanent circuits and have mechanisms to

identify the remote host end of the circuit. The Remote ID field may be used to encode, for instance:

- a "caller ID" telephone number for dial-up connection
- a "user name" prompted for by a Remote Access Server
- 5 - a remote caller ATM address
- a "modem ID" of a cable data modem
 - the remote IP address of a point-to-point link
- a remote X.25 address for X.25 connections

The format of the Agent Remote ID will depend on the type of
10 circuit connected to the relay agent. The only requirement is that the
remote ID be administered as globally unique.

DHCP servers supporting this option MUST return the option
value unchanged in all Offer and Ack responses. DHCP servers MAY
use this option to select parameters specific to particular users,
15 hosts, or subscriber modems. The relay agent MAY use this field in
addition to or instead of the Agent Circuit ID field to select the
circuit on which to forward the DHCP Offer/Ack reply.

DHCP relay agents SHALL NOT modify any existing Agent Remote
ID field in received broadcasted DHCP Discover/Ack packets; such a
20 field may have been added by a circuit bridge.

An Agent Subnet Mask MAY be added by DHCP relay agents which
terminate multiple Logical IP Subnets. It provides the server with
the subnet mask for the LIS on which the relay agent received the
request. (The giaddr field provides the agent's IP host address on that
25 LIS.)

DHCP servers supporting this option MAY copy the Agent Subnet
mask value into the Client Subnet Mask parameter returned to the
host, and SHOULD have a configurable option to do so. DHCP Servers
SHOULD NOT return the Agent Subnet Mask option in the response.

The Agent Subnet Mask option is intended to avoid the duplicate configuration in both the relay agent and the server of the agent's circuit subnet masks. A DHCP relay agent terminating a public data switched network may have thousands of such configured circuits and
5 masks.

DHCP relay agents SHALL remove any incoming Agent Subnet Mask options on received broadcasted DHCP Discover/Request packets from clients. This option is only appropriately added by the relay agent implementing a LIS interface.

10 Although in the preferred embodiment information is added by the relay agent into DHCP packets, this specification is not intended to limit the scope of the invention to the DHCP protocol. This invention applies equally to any application in which the relay agent adds information to client/server packets for use by the relay agent,
15 other relay agent(s), servers, and/or clients.

The present invention may be embodied in other specific forms without departing from the spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive.

20 What is claimed is:

1. A method of relaying DHCP request and response packets by a relay agent between a client and a server, the method comprising the steps of:
 - sending, by the client, a DHCP request packet; and
- 5 inserting, by the relay agent, information into the DHCP request packet to form a modified DHCP request packet.
2. The method of claim 1 further comprising the steps of:
 - 10 using, by the server, the information from the modified DHCP request packet;
 - sending, by the server, a DHCP response packet including the information inserted by the relay agent; and
 - 15 using, by the relay agent, the information from the DHCP response packet.
3. The method of claim 1 wherein the information is a source identifier.
4. The method of claim 2 wherein using, by the relay agent,
 - 20 comprises the steps of:
 - determining, from the source identifier, a destination of the DHCP response packet; and
 - sending the DHCP response packet to the destination.
- 25 5. A relay agent for relaying DHCP request and response packets between a client and a server, the relay agent comprising:
 - a client interface for receiving DHCP request packets from the client;

a relay agent DHCP processor responsive to the client interface for inserting information into the DHCP request packets to form modified DHCP request packets; and

- 5 a server interface responsive to the relay agent DHCP server for sending the modified DHCP request packets to the server.

6. The relay agent of claim 5 wherein the relay agent DHCP processor is further responsive to the server interface for receiving DHCP response packets including the information inserted by the
10 relay agent and for using the information to determine a destination for the DHCP response packets.

7. A server for processing a DHCP request packet containing information inserted by a relay agent, the server comprising:

- 15 a receiver for receiving the DHCP request packet;
a server DHCP processor responsive to the receiver for extracting the information and for processing the DHCP request packet; and

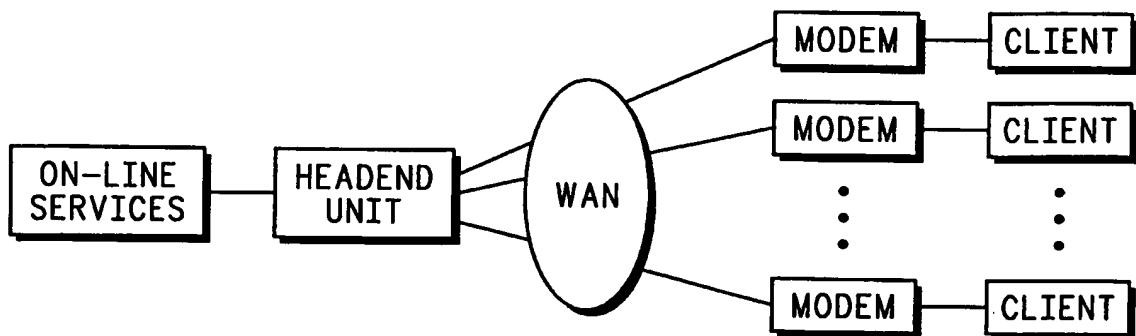
20 a transmitter for sending a DHCP response packet including the information inserted by the relay agent.

8. A system for routing DHCP packets comprising:

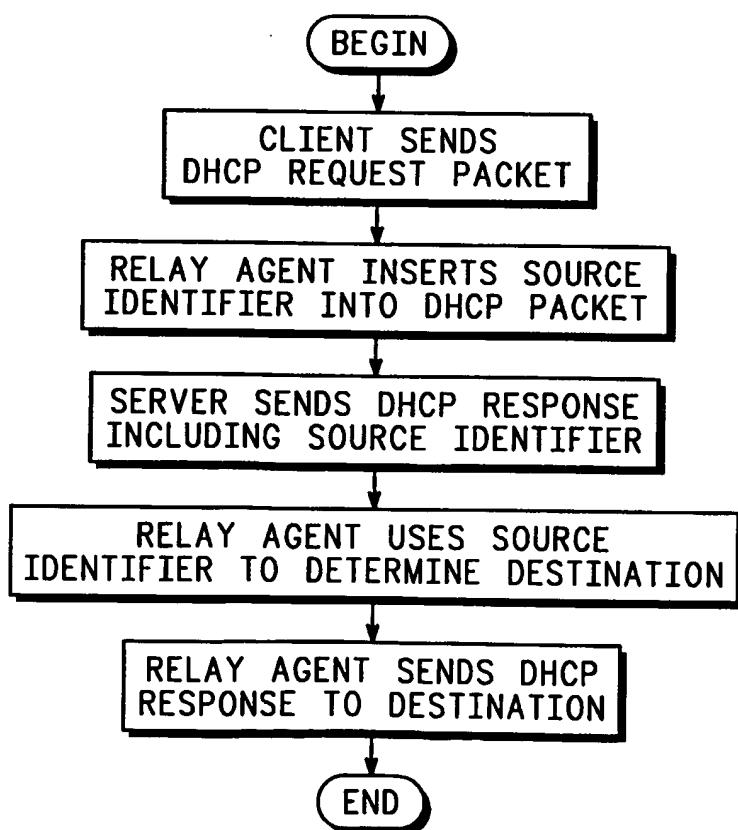
- a client for generating a DHCP request packet;
a relay agent for receiving the DHCP request packet and for
25 inserting information into the DHCP request packet to form a modified DHCP request packet; and
a server for receiving the modified DHCP request packet.

9. The system of claim 8 wherein the server, upon receiving the modified DHCP request packet, generates a DHCP response packet containing the information from the modified DHCP request packet.
- 5 10. The system of claim 9 wherein the relay agent, upon receiving the DHCP response packet, uses the information to determine a destination for the DHCP response packet.

1/2

***FIG. 1***100

—PRIOR ART—

FIG. 2

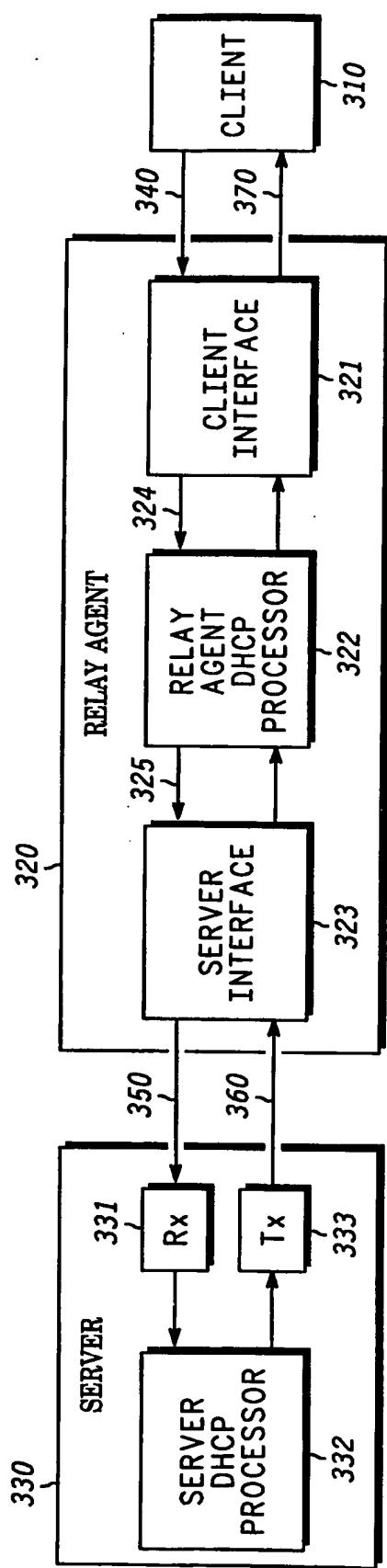


FIG. 3
300

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/22006

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04J 3/02, 3/14; H01J 13/00
US CL :370/242, 245, 252, 402; 395/200.5, 200.52, 200.54, 200.75

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/242, 245, 252, 402; 395/200.5, 200.52, 200.54, 200.75

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS search terms: Dynamic Host Configuration Protocol, DHCP, client, server, interface, relay agent, request packet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,557,748 A (NORRIS) 17 SEPTEMBER 1996, col. 9 line 55 to col. 10 line 40, and col. 11 lines 31-67.	1-10
A, E	US 5,717,860 A (GRABER ET AL) 10 FEBRUARY 1998, see entire document.	1-10
A, E	US 5,724,510 A (ARNDT ET AL) 03 MARCH 1998, see entire document.	1-10

Further documents are listed in the continuation of Box C.

See patent family annex.

Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	
"B"	earlier document published on or after the international filing date	"X"
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"
"O"	document referring to an oral disclosure, use, exhibition or other means	
"P"	document published prior to the international filing date but later than the priority date claimed	"Z"

Date of the actual completion of the international search

29 MARCH 1998

Date of mailing of the international search report

24 APR 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

Douglas Olms

Telephone No. (703) 305-4703

